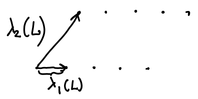
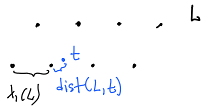
I Определения

– $uSVP_\gamma$ (unique SVP/уникальный SVP): для решётки L, заданной базисом B, такой что $\lambda_2(L) > \gamma\lambda_1(L)$, найти $v \in L\setminus\{0\}$: $\|v\| = \lambda_1(L)$



– BDD_γ (bounded distance decoding / декодирование с огр. расстоянием) : для решётки L, заданной базисом B, и t, т.ч. $dist(L,t) < \frac{1}{\gamma}\cdot\lambda_1(L)$, найти $v \in L$ – ближайший к t.



Замечание $uSVP_\gamma$ сводится к версии поиска Approx SVP_γ
BDD_γ ——— // ——— Approx CVP_γ

В этой лекции мы покажем, что задачи $uSVP_\gamma$, BDD_γ, SVP_γ (версия принятия решений) сводятся друг к другу с poly(n)-потерями (в пар-ре γ), где n - ранг решётки. А именно,

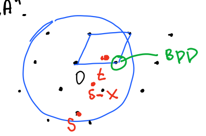
II SVP редуцируется

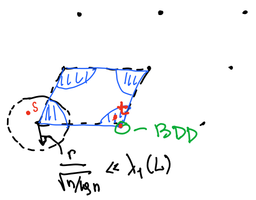
Теорема 1 $\forall \gamma > 2\sqrt{\frac{n}{\lg n}}$, $\exists$ редукция от SVP_γ к $BDD_{\frac{\gamma}{\sqrt{\frac{n}{\lg n}}}}$.

◁ Вход: (B, r) - задача SVP_γ (решить $\lambda_1(L(B)) \le r$ или $\lambda_1(L(B)) > \gamma\cdot r$)
"да" / "нет"

Повторить poly(n)-раз
1) выбрать $s \xleftarrow{\$} B\left(0, r\cdot\sqrt{\frac{n}{\lg n}}\right)$
2) вызвать BDD-оракул для $t = s \bmod P(B)$

Если BDD оракул всегда возвращает $t-s$, вывод "нет", иначе "да".





Случай 1 Если $\lambda_1(L) > \gamma\cdot r$ ("нет"):
$dist(t,L) = dist(s,L) = r\cdot\sqrt{\frac{n}{\lg n}} < \frac{\lambda_1(L)}{\gamma}\cdot\sqrt{\frac{n}{\lg n}}$ – валидный вход для $BDD_{\frac{\gamma}{\sqrt{\frac{n}{\lg n}}}}$ оракула.
Кроме этого, $\frac{\gamma}{\sqrt{\frac{n}{\lg n}}} < \frac{1}{2} \Rightarrow \exists$ единственное решение $t-s$,

Случай 2 $\lambda_1(L) \le r$ ("да").
Положим x, т.ч. $\|x\| = \lambda_1(L)$. Тогда с вероятностью $\frac{1}{poly(n)}$ $\|s-x\| \le d\sqrt{n/\lg n}$
$\Rightarrow$ BDD оракул не сможет ответить корректным $t-s$ с в-тью $\geq \frac{1}{2}$.
После poly(n) запусков, в-ть того, что BDD оракул ответит корректным $t-s$ $\le 2^{-\Omega(n)}$

Лемма (док-во самостоятельно) $\exists x \in \mathbb{R}^n$, т.ч. $\|x\| \le d$. $\exists$ $s \xleftarrow{\$} B(0, d\sqrt{n/\lg$
Тогда с в-тью $\delta > \frac{1}{n^c}$, $c=\Theta($
$\|s-x\| \le d\sqrt{n/\lg n}$

III BDD редуцируется к uSVP

Теорема 2 $BDD_{2\gamma}$ редуцируется к $uSVP_\gamma$

◁ Вход: (B, t) т.ч. $\mathrm{dist}(B,t) < \frac{\lambda_1(L)}{2\gamma}$.

Положим $b \in L$ – ближайший к t, $\mathrm{dist}(b,t) = d$. Положим d известно (угадано).

$$B' = \left[\begin{array}{c|c} B & t \\ \hline -0- & d \end{array}\right] \in \mathbb{Z}^{(n+1)\times(n+1)}$$

$B' \subseteq \mathbb{Z}^2$
$B \subseteq \mathbb{Z}$

Вызываем uSVP оракул на B'. Пусть $\begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$ – выход uSVP.

Вернуть $(s_1 + t)$ – решение BDD.

<u>Корректность</u>: B' – решетка uSVP, т.к. $\begin{pmatrix} t-b \\ d \end{pmatrix} \in L(B')$ и $\left\|\begin{pmatrix} t-b \\ d\end{pmatrix}\right\| = \sqrt{d^2+d^2} = \sqrt{2}\cdot d < \frac{\lambda_1(L)\cdot\sqrt{2}}{2\gamma} = \frac{\lambda_1(L)}{\sqrt{2}\gamma}$.

Покажем, что другие вектора в L', имеют норму $\geq \lambda_1(L)/\sqrt{2}$. (∀ вектора, не паралл. $\begin{pmatrix} b-t \\ d\end{pmatrix}$)

Рассмотрим $\left\|\begin{matrix} c-xt \\ xd \end{matrix}\right\|$ для некоторого $c \in L$, $c \neq d\cdot b$, $d \in \mathbb{Z}$

$$\left\|\begin{matrix} c-xt \\ xd \end{matrix}\right\|^2 = x^2d^2 + \|\underbrace{c - xb}_{\neq 0,\ \in L,\ \|c-xb\| > \lambda_1(L)} + x\overbrace{(b-t)}^{d}\|^2 > x^2d^2 + (\lambda_1(L) - xd)^2 \qquad (\text{т.к. } \|a+b\|^2 > (\|a\| - \|b\|)^2)$$

$$= \underbrace{2x^2d^2 + \lambda_1(L)^2 - 2\lambda_1(L)x\cdot d}_{\text{выражение минимизируется при}} \geq \frac{\lambda_1^2(L)}{2} + \lambda_1^2(L) - \lambda_1^2(L) = \frac{\lambda_1^2(L)}{2}$$

$$4xd^2 - 2\lambda_1(L)d = 0$$
$$2xd - \lambda_1(L) = 0$$
$$x = \frac{\lambda_1(L)}{2d}$$

▶

IV Дуальные решётки

<u>Опр-ие</u> Для решётки L определим $\hat{L}$ – дуальную к L как

$$\hat{L} = \{\hat{b} \in \mathrm{Span}_{\mathbb{R}} L : \ \forall b \in L,\ \langle b, \hat{b}\rangle \in \mathbb{Z}\}.$$

<u>Примеры</u>: $\widehat{\mathbb{Z}^n} = \mathbb{Z}^n$
$\widehat{(2\cdot\mathbb{Z}^n)} = \frac{1}{2}\mathbb{Z}^n$

<u>Свойства</u>

1) B – базис L, то $\hat{B} = B\cdot(B^T\cdot B)^{-T}$ – базис $\hat{L}$.
Если B – кв. матрица, то $\hat{B} = B^{-T}$

◁ $\hat{B}\cdot\mathbb{Z}^n \subseteq \hat{L}$, т.к. $\forall b \in L: b = B\cdot x$ $(x \in \mathbb{Z}^n)$ и $\langle Bx, \hat{B}y\rangle = x^T \underbrace{B^T\cdot B\,(B^T\cdot B)^{-1}}_{Id}\cdot y = x^T\cdot y \in \mathbb{Z}$ $(y \in \mathbb{Z}^n)$

обратно, ∀ $\hat{b} \in \hat{L}$, $\hat{b} = \hat{B}\cdot y$ для $y \in \mathbb{R}^n$, т.к. $\mathrm{Span}_{\mathbb{R}}\hat{B} = \mathrm{Span}_{\mathbb{R}} B$

По опр-ию дуальной решётки $B^T\cdot\hat{b} \in \mathbb{Z}$
$\qquad \shortparallel$
$$\underbrace{B^T\cdot B\,(B^T\cdot B)}_{Id}{}^{-1}\cdot y \in \mathbb{Z}^n \Rightarrow y \in \mathbb{Z}^n \qquad ▷.$$

2) $\widehat{(\hat{L})} = L$ (упр-ие)

3) $\det(\hat{L}) = \frac{1}{\det(L)}$ (упр-ие)

4) $L_1, L_2 \subseteq \mathbb{Z}^d$, то $\widehat{L_1 + L_2} = \hat{L}_1 \cap \hat{L}_2$

5) $B = QR$. Тогда $\hat{B}\cdot J = QJ\,(JR^{-T}J)$ $\quad J = \begin{bmatrix} & & 1 \\ & ⋰ & \\ 1 & & \end{bmatrix}$ – обращает порядок векторов

◁ (случай кв. B): $B = QR$
$B^{-1} = R^{-1}\cdot Q^T$
$B^{-T} = Q\cdot R^{-T} = \hat{B}J = Q(R^{-1}J)$ ▶

6) Transference $\quad 1 \leq \lambda_i\cdot\hat{\lambda}_i \leq n$

◁ $\exists v: \|v\| = \lambda_1$; $\ast$ $\underbrace{x_1, \dots, x_n}_{\text{лин. независ.}} \in \hat{L}$; $\exists i:$ $\langle x_i, v\rangle \neq 0$

$\langle x_i, v\rangle \in \mathbb{Z} \setminus \{0\}$. ▶

7) $\lambda_1(L) \cdot \lambda_1(\hat{L}) \leq n$

◁ $\lambda_1(L) \leq \sqrt{n} \cdot (\det L)^{\frac{1}{n}}$ (Минковский)

$\lambda_1(\hat{L}) \leq \sqrt{n} \cdot (\det L^*)^{\frac{1}{n}} = \sqrt{n} \cdot \left(\frac{1}{\det L}\right)^{\frac{1}{n}}$ ▶

V uSVP сводится к SVP

Теорема 3 $\forall \gamma \leq poly(n)$ $uSVP_\gamma$ сводится к $SVP_{\frac{\gamma}{1+\varepsilon}}$, $\varepsilon > 0$.